DEPARTMENT OF THE TREASURY
FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING

FINANCIAL FRAUD INSTITUTE

TRAINING DEVELOPMENT

**NATIONAL CYBERCRIME TRAINING PARTNERSHIP (NCTP)
TRAINING DEVELOPMENT PLAN FOR TECHNOLOGY CRIME
INVESTIGATORS**

This document was developed by the National Cybercrime Training Partnership (NCTP) as a recommended and approved training hierarchy for the development technology crime investigators. NCTP recommends four levels of progressively more technical training, the details of which are described hereafter.

Module I
The First Responder

The student will understand the role technology plays in criminal activity, the different types of technology they are likely to encounter during criminal investigations and the techniques required to properly seize digital evidence.

Prerequisites: This course is open to law enforcement and personnel tasked with the examination of digital evidence. No previous computer experience is required to attend.

1. The student will understand how crimes involving technology are committed and will be familiar with the various categories of crimes involving the use of technology.

2. The student will be able to recognize hardware and software typically encountered in crimes involving technology.

3. The student will become familiar with observation/patrol techniques specific to technology crime.

4. The student will have a working knowledge of standard evidence protocols and procedures with respect to chain of custody, security, preservation, handling, storage, and retrieval of digital evidence. (Bag and Tag)

5. The student will understand how a digital crime scene differs from a traditional crime scene and will understand how to mitigate damages to digital evidence.

6. The student will have a working knowledge of the use and an understanding of the Officer Safety principles associated with digital evidence. (Booby Traps, Bio and Environmental Hazards, and Electricity)

7. The student will be aware of and understand how to use internal and external resources to properly secure and process a digital crime scene.

8. The student will have a working knowledge of high tech community relations and crime prevention.

9. The student will understand jurisdiction issues and investigative resources specific to state, local, and federal agencies related to technology crimes.

10. The student will understand the criminal and civil implications associated with the handling of digital evidence.

Module II
Search Warrant Execution

The student will be provided with a background in the preparation, planning and execution of a search warrant involving the seizure of digital evidence.

Prerequisites: This course is open to law enforcement and personnel tasked with the examination of digital evidence. The student should have successfully completed the first responder course. Completion of search warrant preparation and investigator courses are highly recommended.

1. The Student will be able to develop a Raid Plan which should include the following:
   a. Emergency procedures / Backup plans
   b. Officer Safety / Environmental hazards
   c. Interagency relationships/Responsibilities
   d. Defining the scope and parameters of the search
   e. Crime Scene control of personnel
   f. Deportment
   g. Intelligence dissemination
   h. Destructive actions / reactions
   i. How to gain physical access to sites/evidence
   j. Team assignments

2. The student will understand the purpose of a raid briefing specific to issues associated with the seizure of digital evidence.

3. The student will understand how to properly secure a digital crime scene physically and electronically, including:
   a. Evaluate communications activity
   b. Evaluate factors that could destroy electronic evidence (i.e. magnets, radios, etc.)
   c. Secure and separate witnesses and suspects
   d. Determine if any data destruction processes are on-going, and take proper action to neutralize

4. The student will understand how to assess and organize a digital crime scene for processing.
   a. Basic system identification (how to tell when you're over your head .... even if you don't think you are)
   b. Factors associated with crime scene assessment (what is relevant and what is not)
   c. Proper organization of the crime scene(s)
   d. Difference between processing techniques for stand-alone/personal and network/commercial crime scenes.

5. The student will be able to demonstrate proper digital evidence handling to include:
   a. Photograph screen, connections, status of system
   b. Properly identify, tag, document, seize, package, and transport hardware, software, and media
   c. Use of technical equipment by law enforcement at search warrant site
   d. Other forensic evidence (fingerprints on disks, etc.)
   e. Other related evidence (ie. notes diaries, manuals, and documentation).
   f. Seizure toolkit/supplies including: storage media, examination software, hand tools, specialized equipment, proper storage containers, etc.
   g. Video recording devices in use by the target
   h. Law enforcement use of video to document a crime scene
   i. Choosing a proper shut down procedure

6. The student will understand the issues of on-scene interviews, including:
   a. Who to interview (e.g. system administrator)
   b. Who should conduct the interview
   c. What questions to ask
   d. Dealing with technical jargon

7. The student will be knowledgeable about search warrant return procedures for appropriate jurisdictions.

Module III
Investigative Considerations in Technical Crime Investigations

The student will receive detailed instruction regarding investigative tactics in technology-related crimes and practical exercises in all aspects of technology investigations.

Prerequisites

This block of training assumes the student is an experienced criminal investigator and has completed the First Responder Course of this series.

I. Case Creation

Identify the steps required to properly initiate a case involving digital evidence, including:

A. Classification of the investigation
   - a. Determination will be made of the type of crime being investigated. Different investigative approaches will be applied to any of several types of identified crimes, such as:
     - i. Internet / Intrusion
       - (a) Insider/Outsider attacks
     - ii. Financial Crime
     - iii. Pornography / Pedophilia
     - iv. Intellectual Property
     - v. Identity Theft
     - vi. Component Theft
     - vii. Espionage
     - viii. Other
   - b. Consider introduction of Subject/Victim profiling and/or case studies into training module.

B. Determine Role of Computer in suspected activity
   - a. "Victim" of crime (or subject)
   - b. Tool of the crime ("weapon")
   - c. Storehouse of evidence
   - d. Facilitator of criminal activity
   - e. Fruit of the crime

C. Determine Your Authority
   - a. Develop a list of suspected statutory violations
   - b. Determine if joint jurisdiction exists with another agency
     - i. Make appropriate liaison if required or desired
     - ii. Consider International implications

D. Screen case according to prosecution guidelines
   - a. If case initially appears to have low prosecution potential, consider

prosecutorial alternatives:

- i. Civil action
- ii. Asset Forfeiture
    - (a) Criminal
    - (b) Civil
- iii. Parallel proceedings
- iv. Pre-Trial Diversion
- v. Cease and Desist
- vi. Disbarment

II. Investigative Phase

Identify proper investigative steps for the investigator to take in developing a criminal investigation involving digital evidence, to include:

A. Determine elements of proof of violation(s)

- a. Identify initial victims and witnesses
    - i. Determine as much as possible whether victims/witnesses are cooperative or (potentially) hostile
    - ii. Conduct initial interviews of victim/witnesses
    - iii. Usually, suspects are not interviewed at this phase

B. Identify types of appropriate legal actions available for obtaining evidence

- a. Consent searches
- b. Subpoenas
- c. Administrative Summons
- d. Warrants
- e. Court Orders

C. Investigative Techniques (Good Practices and "tricks of the trade")

- a. Pretext calls / Ruse visits
- b. Informant Develop
    - i. System Administrators
    - ii. Contract Administrators
    - iii. Network Providers
    - iv. Other
- c. Technical Issues
    - i. Pen Registers, "sniffers", Title Ill's,
    - ii. How to trace e-mail sources; "spoofing"
    - iii. Other Internet investigative techniques
        - (a) Capture and resolve IP Addresses
        - (b) Chat Room Intervention
        - (c) Instant Messenger
        - (d) ICQ ("I Seek You")
- d. DON'T discount the obvious sources of information
    - i. Internet home pages

- ii. Phone Book / Yellow Pages
- iii. Trace Route
- iv. Phone/Utility records
- v. Trash covers
- vi. Mail Cover
- vii. Government required documents
- viii. Publicly available documents

e. Law Enforcement Sources of Information
- i. NCIC/NLETS
- ii. Local Law Enforcement Sources

f. Commercial Data Services
- i. Info America
- ii. CDB Infotech
- iii. Other

g. Undercover Operations
- i. How to protect the investigator's identity
- ii. Apply DOJ On-Line Investigations Guidelines
- iii. Apply relevant sections of Agency Undercover Operations Guidelines
- iv. Use same principles for Cybercrime Undercover Ops as with traditional Undercover Ops

D. Determine location of evidence (specifically digital evidence)

a. Residence
- i. Be aware of issues regarding third-party consent for searches

b. Office
- i. Be aware of issues regarding third-party consent for searches

c. Off-site
- i. Internet Chat Rooms
- ii. Internet News Groups
- iii. E-Mail providers
  - (a) Be aware of provisions of ECPA and PPA
- iv. Information Service Providers
- v. Off-site data backup
  - (a) Consider legal authority for obtaining evidence maintained by a third party.
  - (b) Physical location of data is a critical venue issue

E. Determine what digital data is time sensitive

a. ISP records

b. Read/unread e-mail

c. Log files and date/time-stamped records

F. Identify System specifications

a. Operating system

- i. Windows (various versions)
- ii. Unix/Linux (or derivitives)
- iii. Proprietary Operating Systems

b. Network status

- i. How to determine network configuration

c. Hardware components

d. Quantity of systems to be seized/analyzed

e. Users / Access controls (password control)

f. Applications

g. Encryption usage

G. Documenting the Investigation

a. Careful attention should be paid to maintaining case log and documenting all investigative procedures.

III. Search Warrant Preparation

Identify the appropriate steps for the investigator to take in preparing to execute a Search Warrant in an environment containing digital evidence, to include:

A. Introduce prosecutor to the case

B. Introduce Forensic Personnel to case

a. Assure that proper roles are defined for each

C. Review of types of evidence acquisition

a. Consent Searches

- i. Should consent be signed?
- ii. Assure that consent is very specific for items obtained
- iii. Consent should also be specified for network access (and documented)
  - (a) Does consent for Internet access include consent to read e-mail? Not unless specified.
- iv. Have a strategy for accessing data after consent is given.
  - (a) Will a forensic specialist be available for the consent search?
  - (b) Who will actually do key entry on consented system?
  - (c) Other

b. Various types of subpoenas

- i. Assure that same level of specificity is defined for subpoenas as for warrants
- ii. The purpose and methodology of gaining Grand Jury subpoenas

D. Preparation of affidavits

a. Articulate probable cause that:

- i. A crime has been committed

ii. Digital evidence is located at specified location

iii. Associate the digital evidence with the crime

iv. Associate the digital evidence with a person/suspect

v. Be specific enough to cover all legal requirements, and general enough to avoid the exclusion of relevant evidence

b. Specific list of items to be seized

i. Include everything required to conduct an effective forensic examination

(a) Discuss beforehand with the individual responsible for analysis

(b) Will seizure include peripheral devices, system documentation, etc.?

ii. Affidavit should specify whether physical evidence will be seized or only data

(a) This should be discussed and determined with Prosecutor consideration

(b) Try to prepare affidavit to allow physical seizure unless precluded by Judge/Magistrate

iii. DO NOT be overly ambitious. Take only what you intend to analyze. Taking more than you need results in excessive paper work, storage problems, and a public relations problem.

iv. Avoid in affidavit/warrant - if possible - any reference to time constraints on the return of the evidence.

(a) If time restraints are required, assure that they provide a reasonable amount of time for the effective analysis of the evidence.

v. Assistance in preparation of affidavits can be provided by:

(a) Prosecutor

(b) Agency Legal Counsel

(c) Experienced investigators

(d) DOJ Guidelines for Computer Search and Seizure

E. Determine level of expertise required at search site

a. “Tag and bag” may require few or no computer investigative specialists.

b. Imaging or file copying will require trained specialists

c. Determine if consultants are required

i. Especially important for proprietary systems

ii. Must be specified in affidavit

F. Determine number of people needed at search site

a. Depends on size of organization being searched

b. Depends on scope of search and number of items to be seized

G. Obtain cooperation of local police agencies

a. They can provide site security

b. They probably have better feel for local environment
c. Traffic control

H. Determine time of day / day of week appropriate for search
a. After normal business hours
b. On weekends?
c. A potential problem with this is that systems experts (non-suspects) will not be available for technical assistance.

Module IV
Forensic Examinations - Digital Evidence

The student will gain the knowledge and skills necessary to identify and seize electronics evidence associated with criminal investigations.

SECTION I

BASIC KNOWLEDGE

1. Have an understanding of the history of forensic science.
2. Have a working knowledge of how digital evidence differs from other forensic science disciplines.
3. Have a working knowledge of standard evidence rules with respect to chain of custody, security, preservation, handling, storage, and retrieval.
4. Have working knowledge of Internet for research and technical assistance (Listservs, newsgroups)

HARDWARE

1. Be familiar and have an understanding of the workings of an Intel based IBM compatible personal computer (PC) from a hardware standpoint.
    a. Motherboards
        i. board types
        ii. chipsets
        iii. memory slots
        iv. video and graphics cards
        v. expansion slots (PCI, ISA, AGP)
            1. expansion boards
    b. Input/Output
        i. DMA, IRQ, memory addresses
    c. Controllers
        i. IDE, SCSI, EIDE,
    d. Communication ports
        i. Serial
        ii. Parallel
        iii. USB
        iv. PCMCIA
        v. PS2
        vi. Infrared
        vii. RJ45
        viii. RJ I I (modem)
        ix. Video input/output
        x. Audio digital
        xi. Headphone jack
        xii. Audio line in/out

xiii. Keyboard
xiv. Pointing devices
e. Power supplies
i. UPS
ii. Different watt rating
iii. Power adapters
f. Memory
i. RAM types
ii. EEPROM (motherboard)
iii. Onboard memory
(a) video
(b) microprocessor
iv. Flashcards
g. Storage
i. Fixed and Removable
ii. Hard drives (types, capacities)
iii. DVD RAM/ROM
iv. Floppy
v. Jaz
vi. CD-ROM
vii. CDR
viii. CD-RW
ix. Zip
x. Magneto-optical
xi. Tape
h. Computer BIOS
i. CMOS (upgrade)
ii. Limitations, ie. Hard drive size
iii. Boot order
iv. Date and time
v. Battery
vi. Dynamic drive overlays
vii. Passwords and workarounds
i. Security Devices
i. Biometrics

SECTION 11 - DISK STRUCTURE

1. Physical geometry
a. cylinders, heads, sector
b. low level format
c. last cylinder
2. Logical
a. master boot record

  b. compression
  c. partition table
  d. diagnostic partition
  e. boot record
  f. file allocation table (12, 16, 32, NTFS)
  g. sectors and clusters, relative vs. physical
  h. Directory(root, sub)
    i. Size
    ii. Location
    iii. Contents of directory entry
    iv. Long filenames
3. Data area
  a. How are files saved (creation, saving, fragmentation)
  b. Slack space (RAM, file)
  c. File deletion
  d. Unallocated space
  e. Hidden partitions/data
  f. File attributes
  g. Bad clusters

SECTION III - BOOT SEQUENCE

1. Have a working knowledge of what takes place during boot sequence

SECTION IV - OPERATING SYSTEMS

1. Have a working knowledge of the following OS's: DOS, Windows
  a. Versions
  b. File systems
  c. Commands
  d. GUI

2. Have familiarity with OS features
  a. Windows registry
  b. Batch files
  c. INI files
  d. Memory management
  e. Swap file
  f. Remote file systems (drive mapping)

SECTION V - FORENSIC EXAMINATION CONCEPTS

1. Working knowledge of forensic tools
   a. Write blockers
   b. Imaging software and procedures (time considerations)
   c. Data transfer and procedures (copy)
   d. Media verification (CRC, hash, MD5)
   e. Unerase utilities
   f. Text string searchers
   g. File viewers (header/footer searches)
   h. Graphic search utilities
   i. Directory listings and catalogs
   j. Uncompression utilities
   k. Password recovery
   l. Encryption/decryption tools
   m. Disk/hex editors
   n. Network utilities (traceroute, nslookup, Internic)
   o. Cache rebuilders
   p. System checking utilities
   q. Slack extraction/viewers
   r. E-mail/newsgroup searching tools
   s. Data hiding tools (steganography)
   t. Common commercial software (word processors, spreadsheet, database)
   u. Presentation software
   v. Graphic editors
   w. Media sterilization tools and procedures
   x. CD writing tools
   y. Virus software
   z. Tape backup tools

SECTION VI - SCIENTIFIC METHODOLOGIES

1. Working knowledge of verification/validation procedures
   a. Examiner documentation (SOP,s)
   b. Testing log
   c. Familiarity with national, international standards and working group products.

2. Working knowledge of internal review procedures

SECTION VII - REPORTING AND PRESENTATION

1. Elements to include in forensics report
2. Discovery/FOIA issues
3. Expert vs. non-expert testimony (qualification requirements)
4. Prosecutor education (duty vs. dedicated)
5. Presentation of technical information
6. Court room preparation and types of exhibits

SECTION VIII - EVIDENCE DISPOSITION

1. Working knowledge of wiping standards (NSA, DOD etc.)

Development Team - First Draft of the Field Forensics Training Outlines for Law Enforcement

Kenneth Broderick
Special Agent
Bureau of Alcohol, Tobacco and Firearms
Mr. Broderick, an investigator for ATF for the past eight years, is currently serving as the Project Officer for the ATF computer forensics program. He has completed the basic and advanced Computer Investigative Specialist 2000 programs at the Federal Law Enforcement Training Center. In addition, Mr. Broderick has completed training in Linux and is conducting evaluation testing on Linux examination tools. He has also completed Advanced Internet Investigations instruction at SEARCH, Inc.

Don Cavender
Supervisory Special Agent
Computer Analysis and Response Team
Federal Bureau of Investigation
Mr. Cavender is currently the CART program manager for all FBI offices West of the Mississippi river. For six years, he has conducted computer forensic and high-tech investigations for the FBI including one year as the case agent for the Innocent Images National Initiative against online child exploitation. Mr. Cavender holds a B.A. in industrial design with an emphasis on computer graphics. His teaching assignments include FBI new agent and in-service training and CART basic and advance instruction.

Fred B. Cotton
Director, Training Services
Systems and Technology Program
SEARCH, Inc.
Mr. Cotton directs Training Services at SEARCH's National Criminal Justice Computer Laboratory and Training Center and provides technical assistance and training to criminal justice agencies nationwide in the field of information systems including assistance in the investigation of computer crimes and the examination of seized microcomputers.. In addition to his duties at SEARCH, he is currently a Reserve Police Officer with the Yuba City (California) Police Department where he is assigned to the Sacramento Valley High-Tech Crimes Task Force. He is a Specialist Reserve Officer with the Los Angeles (California) Police Department where he is assigned to the Organized Crime and Vice Division and, he is an Adjunct Professor with the University of New Haven in the Computer Forensic Professional Certificate Program.

Carlton Fitzpatrick
Supervisory Criminal Investigator
Chief, Financial Fraud Institute
Federal Law, Enforcement Training Center - Department of Treasury
Mr. Fitzpatrick has been involved in computer-related investigations since 1978 and has served as high-tech crime investigations trainer and training manager since 1984.

Barron Fong
Supervisory Special Agent
Internal Revenue Service - Criminal Investigation Division
Mr. Fong, based in the San Francisco office of IRS-CID, has served in that capacity for 19 years. His duties include the management oversight responsibilities for the IRS-CID Computer Investigative Specialists located throughout field offices nationwide. He has also been involved with the development and coordination of various training programs for the Treasury Department's CIS2000 initiative, which includes personnel from the BATF, Treasury-IR, Customs and USSS. Mr. Fong participates in number of task forces including the Regional Electronics Computer Intelligence Task Force, the Sacramento Valley Hi-Tech Crime Task Force, and the San Diego Regional Computer Forensic Lab.

David C. Good
Technical Enforcement Officer
Technical Support Division
Bureau of Alcohol, Tobacco and Firearms
Mr. Good has completed the Treasury Computer Investigative Specialist program at the Federal Law Enforcement Training Center and is a Master Certified Netware Engineer. Mr. Good currently provides engineering services for the ATF Computer Forensics Section and recently completed the successful implementation of a Nationwide Enterprise Systems Architecture to include 5000 workstations, network infrastructure, print services, maintenance, installation and support services.

John Gosser
Course Developer/Instructor
Computer Sciences Corporation
Defense Computer Investigations Training Program
Mr. Gosser is employed at Computer Sciences Corporation as a course developer and instructor for the Defense Computer Investigations Training Program (DCITP). He is a recently retired Special Agent from the Defense Criminal Investigative Service (DCIS) where he was the Computer Fraud Program Director. In that position, he began and managed the DCIS computer forensics program and the intrusion investigations program. Mr. Gosser has over 15 years experience in forensic media analysis and computer related investigations. Prior to his federal service, Mr. Gosser was employed by the Colorado State Patrol and the Oklahoma State Bureau of Investigation as a sworn law enforcement officer.

Sam Guttman
Assistant Inspector in Charge
Forensic and Technical Services Division
US. Postal Inspection Service
Mr. Guttman has been involved with computer forensics for over ten years as both a field agent and laboratory manager. Mr. Guttman was instrumental in establishing the first Digital Evidence unit in the Postal Inspection Service. He now oversees the agency's digital evidence initiative consisting of laboratory and field resources.

Kathleen M. Higgins
Director
Office of Law Enforcement Standards
National Institute of Standards in Technology
Ms. Higgins holds a B.S. in chemistry from the University of Rhode Island and a Master's degree in Forensic Chemistry from Northeastern University, Boston, MA. Her professional experience includes over fifteen years as the analyst of record in more than 2000 criminal and civil cases; supervision of the Criminalistic Section of the Massachusetts State Police Crime Laboratory; the founding and directing of K-Chem Laboratories, a private laboratory providing testing and evaluation of evidentiary materials; management and coordination of graduate and undergraduate forensic science programs at Northeastern University; and, materials research and development related to security, environmental and toxicological issues for the U.S. Postal Service.

Shlomo Koenig
Deputy Sheriff
Rockland County Sheriff Department
Computer Crimes Unit
Mr. Koenig has served to develop several computer crimes courses and provided instruction for hundreds of law enforcement officers of various New York and New Jersey police departments including the Port Authority of NY/NJ , the Office of Inspector General detectives, and in-service training for Police Academy on the topic of computer crime. Mr. Koenig has completed high-tech training in a number of disciplines and is now a Certified Fraud Examiner (CFE), an IACIS Computer Forensics Certified Examiner, a Certified Crime Prevention Specialist and a New York State Certified Police Training Instructor.

Barry Leese
Detective Sergeant
Maryland State Police
Mr. Leese is a 26 year veteran of the Maryland State Police. He currently holds the position of Commander, Computer Crime Unit. Mr. Leese has received specialized training and has acquired an expertise in computer forensic examinations and computer crime investigations.

Joseph Muldoon
Supervisory Special Agent
Department of Defense
Computer Forensics Investigations Branch
Mr. Muldoon has managed the Computer Forensics Investigations Branch for the past five years. He has worked for the Department of Defense for the past eighteen years after graduating from Boston College in 1981.

Glenn Nick
Senior Special Agent
Assistant Director - Cybersmuggling Center
U.S. Customs Service
Mr. Nick manages the Custom's computer forensic program and supervises the Cybersmuggling Center's Cybercrime Investigative Unit. Mr. Nick has developed computer forensic training and Internet investigative classes for presentation to international law enforcement agencies and U.S. state and local law enforcement agencies. Mr. Nick represents the U.S. Customs Service on the G8 High Tech Crime Subgroup, the World Customs Organization Cybercrime Workgroup, and the Scientific Working Group - Digital Evidence.

Greg Redfern
Special Agent
Naval Criminal Investigative Service
Mr. Redfern has been with the NCIS since 1978. He has been involved with computer investigation training issues since 1997. He was name as the first Director of the Department of Defense Computer Investigations Training Program in May 1998.

Mary Riley
Assistant to Special Agent In Charge
Financial Crimes Division - Electronic Crimes Branch
U.S. Secret Service
Ms. Riley has been assigned as the agent in charge of the Electronic Crimes Branch of the Secret Service Headquarters where she is responsible for the case coordination of all telecommunications and computer network investigations conducted by Secret Service field offices. The branch also coordinates the forensic analysis of computer and telecommunications equipment seized as evidence in all investigations through a team of 150 special agents trained as experts in computer forensics. Ms. Riley has been with the Secret Service since 1987 and holds a bachelor of science degree in computer information management.

Larry Stinson
Investigator and Computer Forensic Examiner
Computer Crimes Unit
Los Angeles County Sheriff's Department
Mr. Stinson has been a law enforcement officer for 21 years. He is a departmental instructor of investigative computer applications and the search and seizure of computers. He has testified as an expert in the areas of counterfeiting, fraud, unlawful access, destruction of data, and computer forensics before the California municipal and superior courts. He is a Microsoft certified systems engineer, and has been formally trained in the science of computer forensics. He is a member of the High Technology Crime Investigation Association.